



Izobraževalni seminar
SVIZ – visoko šolstvo in znanost

VARSTVO OSEBNIH PODATKOV V DELOVNEM RAZMERJU

mag. Polona Štrekelj, Ankaran, 13.9.2021



iDecide

Individuals decide - raising awareness
about data protection rights

Projekt financira Evropska komisija v okviru Splošnega programa »Rights, Equality and
Citizenship Programme 2014 – 2020«.



Vsebina

1. Obdelava osebnih podatkov s sodobnimi tehnologijami (videonadzor, biometrija, e-pošta, internet, telefon, tiskalniki, itd.)
2. Obdelava osebnih podatkov v času boja proti širjenju okužb z virusom SARS-CoV-2
 - delo na daljavo (nadzor zaposlenih, uporaba sodobnih spletnih orodij)
 - preverjanje izpolnjevanja PCT pogojev



Uporaba sodobnih tehnologij

Obdelava OP s pomočjo sodobnih tehnologij (videonadzor, biometrija, GPS naprave, telefon, tiskalniki, e-pošta, internet, aplikacije za delo od doma, videokonferenčni sistemi, itd.)...

... **meja** med službenim in zasebnim **se briše**

... omogoča lahko **prikrit nadzor** zaposlenih **na delovnem mestu** in **pri delu od doma**

... **zakonsko neurejeno področje** (razen videonadzora, biometrije in porabe na službenih telefonih), zato mora delodajalec izhajati iz **splošnih načel varstva osebnih podatkov**, pred tem pa razmisliti:

- ✓ o namenu, ki ga želi doseči (kaj želi z ukrepom urediti oz. katero težavo skuša rešiti)
- ✓ razmisliti, ali je ukrep sploh potreben in sorazmeren glede na namen
- ✓ izbrati najustreznejšo pravno podlago



Uporaba sodobnih tehnologij

... zato naj delodajalec (upravljavec) pred odločitvijo o uporabi sodobnih tehnologij:

1. **izvede oceno učinka** (opredelitev namena, izvedba ocena potrebnosti in sorazmernosti, izvedbe ocene tveganj za posameznike in opredelitev ukrepov za obravnavo tveganj),
2. **vnaprej določi pravno podlago** (najustreznejšo pravno podlago – člen 6(1) Splošne uredbe, ZVOP-1 (videonadzor, biometrija), področna zakonodaja),
3. **zagotovi predvidljivost** (interni akt in seznanitev delavcev)
4. **raje vnaprej omeji kot nadzira** (tehnična sredstva)



Videonadzor

Področna ureditev v ZVOP-1 (74. – 77. člen):

- videonadzor dostopa v uradne službene ali poslovne prostore, če je to potrebno za **varnost ljudi** ali **premoženja**, zaradi **zagotavljanja nadzora** vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela **obstaja možnost ogrožanja zaposlenih (74. in 75. člen ZVOP-1)**;
- **sklep o uvedbi (pisna odločitev z razlogi o uvedbi), predhodno pisno obvestilo zaposlenim in obvestilo ob izvajanju**
- **NIKOLI v garderobah, dvigalih, sanitarnih prostorih!**
- **gre za obdelavo osebnih podatkov tudi če ni snemanja!**
- na delovnem mestu le v izjemnih primerih (če je **NUJNO** potrebno za **varnost ljudi ali premoženja** ali za **varovanje TP/PS**), posvetovanje z **reprezentativnim sindikatom**

Dolžnosti po Splošni uredbi:

- ureditev zunanjega izvajanja, npr. varnostne službe (28. člen)
- vzpostavitev evidence dejavnosti obdelave (30. člen)
- zagotavljanje varnosti (32. člen)
- obveščanje o kršitvah varnosti (33. člen)
- ocena učinka (35. člen)
- vloga DPO (37.-39. člen)
- pravice posameznika!





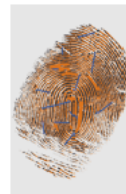
Biometrijski ukrepi

Biometrični podatki – fizične, fiziološke ali vedenjske značilnosti posameznika, obdelane s posebnimi tehničnimi sredstvi, ki omogočajo edinstveno identifikacijo ali avtentikacijo posameznika

- telesne: obraz, prstni odtisi, DNK, mrežnica, šarenica itd.; vedenjske: govor (glas), gibanje, tipkanje itd.

Področna ureditev v ZVOP-1 (78. – 81. člen):

- loči med javnim in zasebnim sektorjem
- javni s.: če so **nujno potrebni** za **opravljanje dejavnosti**, za **varnost ljudi** ali **premoženja** ali za **varovanje tajnih podatkov** ali **poslovne skrivnosti** in je to določeno **v zakonu** (npr. Zakon o potnih listinah), izjemoma lahko tudi za vstop v stavbo in evidentiranje zaposlenih na delu;
- zasebni s.: isti pogoj + **le nad svojimi zaposlenimi**, če so bili **predhodno o tem pisno obveščeni** + **predhodna odločba IP** (soglasje zaposlenih ne zadostuje)



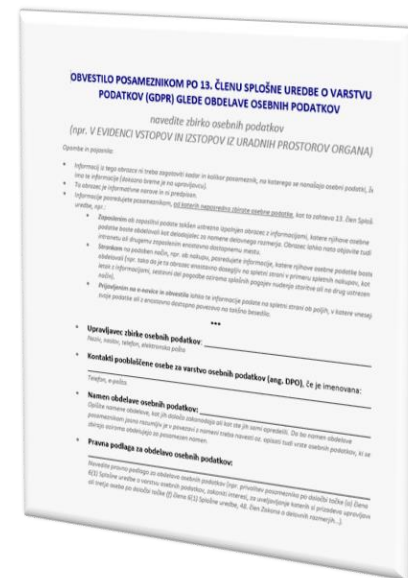


Telefoni in tiskalniki

- **Mobilni / službeni telefoni (139. člen Zakona) o elektronskih komunikacijah): določitev limita v internem aktu**
 - če posameznik prekorači limit, z razčlenjenim računom dokazuje službeno porabo (zakriti, nezakriti RR)
 - če prekoračitve limita ni, naj se ne preverja seznama klicev
- **(Mrežni) tiskalniki /multifunkcijske naprave**
 - **Tudi tiskalniki lahko ustvarjajo zbirke osebnih podatkov uporabnikov – preverite, obvestite zaposlene!**
 - Npr. hramba podatkov o naslovu dokumenta, URL natisnjene spletne stani ipd.
 - če je zasebna poraba problem, je priporočljiv režim limita tiskanja (npr. vezava na uporabniško kartico, x strani glede na delovno mesto), odobritev za povečan obseg tiskanja
 - podobno priporočilo kot pri mobilnih telefonih

OBVESTILO POSAMEZNIKOM PO 13. ČLENU SPLOŠNE UREDBE O VARSTVU PODATKOV GLEDE OBDELAVE OSEBNIH PODATKOV

(obrazec na ip-rs.si)





Elektronska pošta in dostop do interneta

Dopustno tehnično omejevanje vnaprej, ne pa naknadno preverjanje!

- Npr. omejevanje določenih URL naslovov, velikosti in formata priponk
- Pozor pri **preusmeritvah predalov e-pošte!** (NE avtomatskih preusmeritev, priporočljiv avtomatski odgovor)
- vsebina e-pošte – ne pokriva Splošna uredba (sodna odredba)! **seznam obiskanih spletnih strani (vsebina)/prometni podatki o e-pošti po uporabniku = zbirka osebnih podatkov!**
- natančna opredeljenost v internih aktih (izjemno redko, za kakšen namen, katere podatke,...)
- Pozor pri vsebini - komunikacijski zasebnosti (37.člen Ustave RS - tajnost pisem in drugih občil - KD)!
- Primeri neustreznih določb v internih aktih:
 - »Uporaba interneta s strani zaposlenih se lahko nadzira.«,
 - »V okviru rednih vzdrževalnih pregledov ali po naročilu odgovorne osebe informatik pregleduje dostope posameznikov do različnih spletnih naslovov in izdela poročilo pregleda dostopanja do svetovnega spleta.«



Uporaba zasebnih naprav v službene namene (BYOD)

Pred uvedbo priporočljivo izvesti oceno učinkov na varstvo OP.

Gre za analizo tveganj po temeljnih načelih varstva osebnih podatkov:

- **zakonitost** (pravne podlage, zakon, privolitev,...
 - **poseben pomen ima informiranje** – kako in o čem bodo zaposleni obveščeni)
 - vpliv na raven **pričakovane zasebnosti!**
 - veljavnost privolitve v delovno-pravnih razmerjih?
- **sorazmernost** (kateri podatki so nujni)
- **namenskost** (definiranje in omejitev namenov)
- **točnost in ažurnost** (npr. vnašanje podatkov in ustrezna sinhronizacija)
- **zavarovanje** (vidiki informacijske varnosti)
- **pravice posameznika** (katere in kako bodo zagotovljene)
- **roki hrambe** (kako dolgo bodo podatki hranjeni, možnosti dostopa...)



[Smernice o uporabi zasebnih naprav v službene namene \(BYOD\)](#)



... in delo od doma



Informacijski pooblaščenec priporoča, da delodajalci **vneprej ocenijo vsa morebitna tveganja**, ustrezne **organizacijske in tehnične ukrepe navedejo v svojih internih aktih** in z njimi **seznanijo svoje zaposlene**.

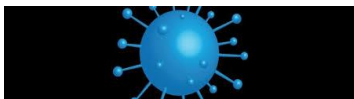
V vsakem primeru morajo delodajalci:

- vpeljati in posodabljati vse **varnostne mehanizme** (antivirusni program, požarni zidovi, filtriranje internetnega prometa, sistem za preprečevanje/prepoznavo nepooblaščenega dostopa,...)
- **zavarovati prenosnike in mobilne telefone z ustrezno avtentikacijo** (2FA, gesla, VPN...);
- opozarjati delavce na **pazljivost pred nepooblaščenim dostopom** (zaklepanje ekrana po določenem času neuporabe ...);
- **vpeljati in izvajati politiko močnih gesel**;
- **ustrezno šifrirati komunikacijo** (e-pošta, internet, telefon ...) in informirati zaposlene, da uporaba zasebne e-pošte ni priporočljiva;
- **pred uporabo pregledati vse prenosne naprave** (USB ključki, zunanji diski ...), da ne vsebujejo škodljivih ali zlonamernih programov (črvi, virusi, trojanski konji ...);
- pri uporabi avdio in video klicev (namesto fizičnih sestankov) **preveriti varnost posamezne aplikacije in priporočiti delavcem uporabo preverjenih programov**;
- **zagotavljati varnost tudi na klasičnih medijih** (npr. papirju).



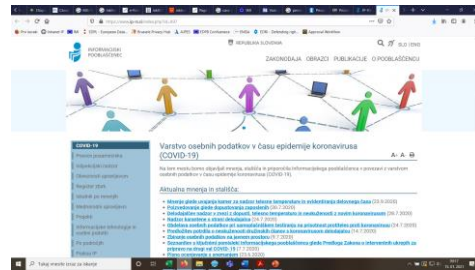
Obdelava osebnih podatkov v času boja proti širjenju okužb z virusom SARS-CoV-2

Širjenje epidemije koronavirusa (COVID-19) je v okviru obdelave osebnih podatkov v delovnih razmerjih prineslo **2 novi dimenziji** :



1. **Sprememba delovnega procesa z izvajanjem različnih oblik dela na daljavo** - oddaljeni dostop zaposlenih do različnih strežnikov (npr. poštnih/datotečnih), aplikacij (npr. spletni klepetalniki) in konferenčnih sistemov (npr. MS Teams, Zoom), kar prinaša številna vprašanja z vidika pravnih podlag obdelave osebnih podatkov in njihove varnosti, predvsem pa z vidika nadzora zaposlenih s strani delodajalca
2. **Uvajanje ukrepov, ki vključujejo obdelavo podatkov o zdravstvenem stanju delavcev** (posebne vrste osebnih podatkov), ki so namenjeni zaščiti življenjskih interesov zaposlenih, podjetja in javnega interesa – ključna je zdravstvena stroka!

...vsa aktualna stališča in mnenja IP v zvezi z varstvom osebnih podatkov v času izrednih razmer zaradi koronavirusa so dostopni na spletni strani <https://www.ip-rs.si>





Izhodišča za obdelavo osebnih podatkov v zvezi z obolelostjo s koronavirusom COVID-19

Tehtanje dveh temeljnih pravic:

pravica do zasebnosti (varstvo osebnih podatkov)



pravica do javnega zdravja

Vsaka obdelava osebnih podatkov = poseg v pravico do zasebnosti... obdelava zdravstvenih osebnih podatkov še toliko bolj!

Zato mora biti obdelava osebnih podatkov:
NUJNA, UPRAVIČENA (UČINKOVITA!) IN SORAZMERNNA

QUARANTINE BREACH!
QUARANTINE BREACH!





Delo na daljavo

Delo od doma – na podlagi sodobnih tehnologij lahko pride do povečanega obsega nadzora nad zaposlenimi s strani delodajalca, iz (vsaj) treh razlogov:

- **spremljanje učinkovitosti zaposlenih** (npr. sledilnik aktivnosti, prikazovanje ekranskih slik računalnika, spremljanje prijave/odjave, aktivnosti na tipkovnici, prometa na internetu, e-pošti itd...s pomočjo programov npr. StaffCop, Teramind, CleverContro, TimeDoctor itd.,
- **spremljanje morebitnih notranjih varnostnih groženj** (spremljanje prometa na internetu, omrežju itd.) ter
- **izvajanje delovnega procesa na daljavo (MSTeams, Zoom,)**





Delo na daljavo

- IP podpira uporabo novih tehnologij, orodij in metod, ki so povezane s pedagoško-izobraževalnim delom v času izrednih razmer v času COVID-19, ki pa mora biti **premišljena, sorazmerna in varna**
- **pred uvedbo katerekoli rešitve IP upravljavcem priporoča izvedbo ocene učinkov na varstvo OP (v kolikor le ta ni obvezna že na podlagi Splošne uredbe):**
 - **določitev namena (člen 5)** - definiranje in omejitvev namenov)
 - **določitev ustrezne pravne podlage zakonitost (člen 6(1), 9(2))** - ustrezna pravna podlaga – ZDR-1, Zakon o visokem šolstvu,... , privolitev?
 - **sorazmernost (člen 5)**- kateri podatki so res nujni za dosego nekega namena
 - **informiranje zaposlenih (člen 13)** - interni akt
 - **točnost in ažurnost (člen 5)**
 - **zavarovanje (člen 32, 24. in 25. člen ZVOP-1)** - vidiki informacijske varnosti, sodelovanje IT službe
 - pogodbeno obdelava (člen 28) – če orodje/tehnologijo zagotavlja zunanji izvajalec
 - **roki hrambe (člen 5)** - kako dolgo bodo podatki hranjeni – omejeno na obdobje izrednih razmer!
 - prenos podatkov v tretje države (člen 46) – določitev zaščitnih ukrepov
 - **pravice posameznika** (katere in kako bodo zagotovljene)



Obdelava osebnih podatkov v okviru preverjanja PCT pogojev

Trenutno v veljavi:

- Odlok o načinu izpolnjevanja pogoja prebolewnosti, cepljenja in testiranja za zaježitev širjenja okužb z virusom SARS-CoV-2 (Uradni list RS, št. 142/21) – **velja do 14.9.2021!**
- Odlok o načinu izpolnjevanja pogoja prebolewnosti, cepljenja in testiranja za zaježitev širjenja okužb z virusom SARS-CoV-2 (Uradni list RS, št. 146/21) – **velja od 15.9.2021 dalje!**
- Odlok o načinu ugotavljanja izpolnjevanja pogojev prebolewnosti, cepljenosti in testiranja v zvezi z nalezljivo boleznijo COVID-19 (Uradni list RS, št. 126/21) ter
- Odlok o začasni omejitvi zbiranja ljudi zaradi preprečevanja okužb s SARS-CoV-2 (Uradni list RS, št. 129/21, 132/21, 135/21, 140/21 in 146/21)



Odlok o načinu izpolnjevanja pogoja prebolevnosti, cepljenja in testiranja za zaježitev širjenja okužb z virusom SARS-CoV-2

Pogoj PCT morajo izpolnjevati („KDO“):

- vsi delavci in osebe, ki na kakršnikoli drugi pravni podlagi opravljajo delo pri delodajalcu, ali samostojno opravljajo dejavnost
- vse osebe, ki so uporabniki storitev ali udeleženi ali prisotni pri izvajanju dejavnosti ali v okoljih v RS,
- razen (izjeme): mlajši od 12 let, osebe, ki pripeljejo otroke v vrtec/1.-3. razred OŠ, osebe, ki spremljajo otroke do 15. leta k zdravniku, učencem/dijakom pri prevozu z JPP, trgovine z osn. življen. izdelki/potrebščinami, pri zagotavljanju javnega reda in miru, varnosti/obrambe, nujne med. pomoči ter zaščite in reševanja



Odlok o načinu izpolnjevanja pogoja prebolewnosti, cepljenja in testiranja za zajezitev širjenja okužb z virusom SARS-CoV-2

- **Dokazila („KAJ“):** PCT pogoj je izpolnjen, če osebe razpolagajo z enim od taksativno navedenih **dokazil** + test HAG za samotestiranje 1x tedensko ali test HAG 1x tedensko (za zaposlene)/test HAG 1x tedensko, če se je uporaba storitve začela v 48 urah od odvzema brisa (za uporabnike storitev)
- **Preverjanje („KAKO“):** organizirajo **odgovorne osebe**, ki izvajajo ali organizirajo opravljanje dela...**z dokazili iz 2. in 6. člena...**in sicer **na vstopnih točkah...**na način kot je določen v Odloku o načinu ugotavljanja izpolnjevanja pogojev prebolewnosti, cepljenosti in testiranja v zvezi z nalezljivo boleznijo COVID-19 (**z aplikacijo ali vpogledom**)



Odlok o načinu izpolnjevanja pogoja prebolewnosti, cepljenja in testiranja za zajezitev širjenja okužb z virusom SARS-CoV-2

- preverjanje izpolnjevanja pogojev – z aplikacijo ali vpogledom v dokazilo (=obdelava osebnih podatkov)
- 38. člen URS - zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov v skladu z drugim odstavkom 38. člena Ustave RS lahko določeno zgolj z zakonom – **vprašanje protiustavnosti (presoja US)**
- **Toda! sprejeti odloki veljajo**, in so jih dolžni spoštovati vsi, na katere se odloki nanašajo - do njihove izrecne razveljavitve s strani US RS ...

pri čemer pa se upravljavci soočajo s celo vrsto vprašanj:



Odlok o načinu ugotavljanja izpolnjevanja pogoja prebolevnosti, cepljenja in testiranja za zajezitev širjenja okužb z virusom SARS-CoV-2

Ugotavljanje izpolnjevanja pogoja PCT poteka na dva načina:

- z aplikacijo za odčitavanje QR kode (NIJZ) ali
- z vpogledom v dokazilo,

pri čemer se istovetnost dokazuje z javno listino.

Vloga **privolitve**? Problematična iz več razlogov – kot pravna podlaga iz člena 9(2)(a) in kot pravna podlaga v razmerju oblast-posameznik

Aplikacija izpiše **podatek o izpolnjevanju PCT pogoja (zeleno/rdeče)**, pri čemer ni razvidno, katerega izmed pogojev oseba izpolnjuje ter **osebno ime in letnico rojstva**.

Aplikacija ne omogoča hrambe podatkov.

Vpogled v dokazilo?



Odlok o načinu ugotavljanja izpolnjevanja pogoja prebolewnosti, cepljenja in testiranja za zajezitev širjenja okužb z virusom SARS-CoV-2

- Na kakšen način organizirati preverjanje izpolnjevanja PCT pogojev, da bo le to skladno s prepisi (glede na to, da bodo posamezniki v praksi predložili vrsto različnih dokazil + evidenčni list za samotestiranje)?
- Preverjanje z aplikacijo ali z vpogledom? V katere podatke?
- Katere evidence z informacijami o izpolnjevanju dokazil smejo voditi upravljavci (za zaposlene, za obiskovalce)?
- ...
- ... sodelovanje z Inšpektoratom za zdravje in MIZŠ (skupna priporočila)...



Hvala za pozornost! 😊

Vprašanja?

polonca.strekelj@ip-rs.si